Amendments to the Drawings:

No amendments are made to the Drawings herein.

Remarks

By the foregoing Amendment, Claim 1 is amended and Claims 18, 20-27 and 32-34 are cancelled. Entry of the amendment and favorable consideration thereof is earnestly requested. Claims 1-6, 9-17 and 29-31 are currently pending.

All claims stand rejected under 35 U.S.C. 103(a) as being unpatentable over Zizzi (U.S. Patent No. 6,185,681) in view of Zimmerman (U.S. Patent No. 6,314,190). Applicant respectfully asks the Examiner to reconsider these rejections in view of the above Amendments and the below Remarks.

The present invention is directed to a system for encrypting data files of application programs which includes a security file for encrypting and decrypting data files and for launching software applications. The invention further operates automatically without user intervention and as an addition to existing applications, whereby said applications need not be modified.

Independent Claim 1

Applicant respectfully submits that there are at least three elements of Claim 1 that are not disclosed, taught or suggested by the cited prior art, or any other prior art of which Applicant is aware.

First, Claim 1 requires an encrypt key for encrypting and decrypting data files, which is itself stored in an encrypted file. Applicant respectfully submits that this is not disclosed, taught or suggested in any way by Zizzi. In Zizzi, all of the encrypt keys (sometimes also referred to in Zizzi as the "key values") are stored in a key table stored on a smart card. As is explained in detail in Zizzi, when a file is to be encrypted or decrypted, an encryption key name or a decryption key name is used to identify the appropriate encryption key or decryption key from the key table stored on the smart card. Once the appropriate encryption key or decryption key is retrieved from the smart card, the file is encrypted or decrypted as appropriate. (see, for example, column 9, lines 20-31; column 10, lines 3-15). There is absolutely no disclosure, teaching or

suggestion to encrypt the encryption keys or the decryption keys (as is evidenced by the fact that there is no discussion as to how the encryption keys or decryption keys would or could be encrypted or decrypted).

Nor would there be any reason to modify Zizzi to so encrypt the encryption keys and decryption keys. The reason the encryption/decryption keys of the present invention are themselves encrypted is because they are stored in a data file which is located on a storage device, which may be accessible to all users of the computer system (including users who might not be authorized to view encrypted data files) and which might be accessible to hackers. However, since the encryption keys and decryption keys of the system described in Zizzi are stored on a smart card, which the user is intended to carry on his/her person and insert into the smart card reader only when that person is using the system, the encryption keys and decryption keys are not accessible to other users of the system or to hackers. As such, encryption of the encryption keys and decryption keys is not necessary.

With respect to the "encryption key name" and the "decryption key name" discussed in Zizzi, these are not encryption keys or decryption keys, but rather merely an identification of which encryption or decryption key stored in the key table on the smart card is appropriate for a particular file. (see, for example, column 9, lines 25-28; "The encryption key name is preferably an alphanumeric descriptor which may be used by the user and/or system administrator for administering the encryption key value." (emphasis added)). Moreover, even if the encryption key name and the decryption key name could be considered to be "encrypt keys" within the meaning of Claim 1, they are not themselves encrypted. Zizzi discloses that the encryption key names and decryption key names may be stored either in the encrypted file's header or the encrypted files table (i.e., on the smart card). However, it is not possible for these locations to be encrypted, or the system could not work as described. For example, if the decryption key name was stored in the encrypted file's header, and the header itself was encrypted as part of the encrypted file, how could one decrypt the header to obtain

the decryption key name (which is used to identify the appropriate encryption key for decrypting the file)? This would be a typical "Catch-22" situation. The system would need to identify the appropriate decryption key to decrypt the header, but the appropriate decryption key cannot be identified until the header is decrypted. The system simply would not work if the header, where the decryption key name is stored, was encrypted with the rest of the file.

Second, Claim 1 requires that the encrypt key be stored in an encrypted file on the storage device. As discussed above, all of the encrypt keys in Zizzi stored in a key table stored on the smart card. As such, Zizzi does not anticipate this element of Claim 1. Moreover, Applicant respectfully submits that it would not have been obvious to have modified Zizzi to arrive at this limitation. This is true because it is one of the main objects of Zizzi to have the encrypt keys stored separately and independently from the remainder of the system (see, for example, column 4, lines 17-20; "It is a further object to provide a document encryption and decryption system which takes advantage of the features of smart cards which are not available from pure on-line security systems.").

Third, Claim 1 requires that the encrypt key be stored together with an application identifier in an encrypted file. Applicant respectfully submits that this is not even remotely contemplated by Zizzi.

With respect to Zimmerman, Applicant respectfully submits that this reference teaches nothing that would, either alone or when combined with Zizzi, anticipate or render obvious the above-identified elements of Claim 1. Indeed, the Examiner cites Zimmerman for completely unrelated teachings.

Independent Claim 29

Claim 29 requires, among other elements, combining the size of a file with a passkey component, selected from a list of possible passkey components, to form a passkey, and using the passkey to encrypt the file. Applicant respectfully submits that there is nothing in the cited prior art, or any other prior art of which Applicant is aware,

that discloses, teaches or suggests such a method for creating a passkey used to encrypt a file.

While both Zizzi and Zimmerman disclose various methods for generating and using encryption keys, neither discloses, teaches or suggests that the size of a file can be used to create a passkey for encrypting that file. Zizzi makes no mention of data size whatsoever, and indeed, it appears that the Examiner is instead citing Zimmerman as teaching this element. However, the only "size" that Zimmerman even touches upon is allowing the user to specify the size of the keys (i.e., the number of bits used to construct the digital key) (see Figures 5A, 5B, 6A-6F; column 9, line 61 - column 10, line 4). There is absolutely no disclosure, teaching or suggestion that the size of a file can be used in any way (never mind being combined with a passkey component selected from a list of possible passkey components) to form a passkey used to encrypt that file.

In view of the above, it is respectfully submitted that claims 1-6, 9-17 and 29-31, all of the claims remaining in the application, are in order for allowance and early notice to that effect is respectfully requested.

Respectfully submitted,

Wesley W. Whitmyer, Jr., Registration No. 33,558
Todd M. Oberdick, Registration No. 44,268
David Chen, Registration No. 46,613
Attorneys for Applicant
ST. ONGE STEWARD JOHNSTON & REENS LLC
986 Bedford Street
Stamford, CT 06905-5619
203 324-6155